(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
22 December 2011 (22.12.2011)

PCT

(10) International Publication Number
WO 2011/157750 A2

(51) **International Patent Classification:**
G06F 21/00 (2006.01)

(21) **International Application Number:**
PCT/EP201 1/059941

(22) **International Filing Date:**
15 June 201 1 (15.06.201 1)

(25) **Filing Language:** English

(26) **Publication Language:** English

(30) **Priority Data:**
61/344,255 18 June 2010 (18.06.2010) US

(71) **Applicant** *(for all designated States except US):* **CARD-LAB APS** [DK/DK]; William Wains Gade 9-14, DK-1432 Copenhagen K (DK).

(72) **Inventor; and**
(75) **Inventor/Applicant** *(for US only):* **NORDENTOFT, Torsten** [DK/FR]; Domaine Des Bois D'Amont, 1850 route Saint Vallier, F-06530 Speracedes (FR).

(74) **Agents: FOGED, Soren** et al; Inspicos A/S, P.O. Box 45, Kogle Alle 2, DK-2970 Heirsholm (DK).

(81) **Designated States** *(unless otherwise indicated, for every kind of national protection available):* AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PE, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) **Designated States** *(unless otherwise indicated, for every kind of regional protection available):* ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Declarations under Rule 4.17 :

— *of inventorship (Rule 4.1 7(iv))*

Published:

— *without international search report and to be republished upon receipt of that report (Rule 48.2(g))*

(54) Title: A COMPUTER ASSEMBLY COMPRISING A COMPUTER OPERABLE ONLY WHEN RECEIVING A SIGNAL FROM AN OPERABLE, PORTABLE UNIT

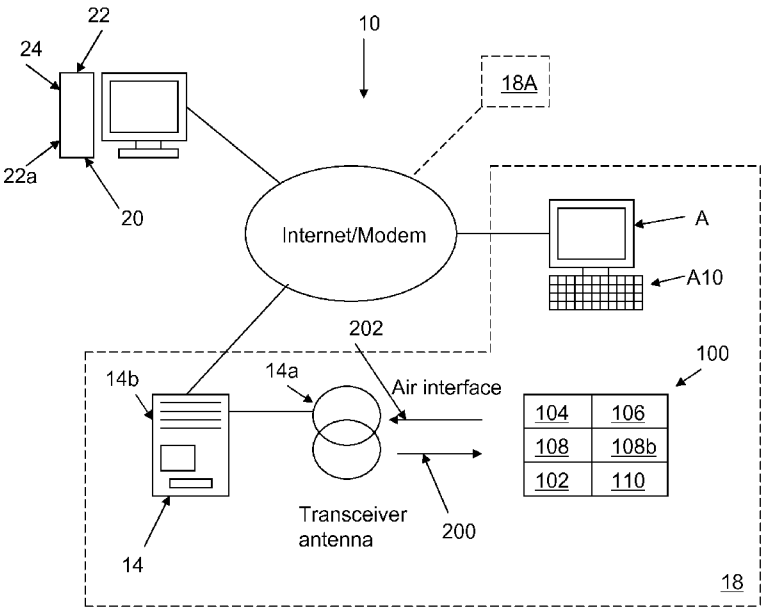


Figure 1

(57) Abstract: A computer assembly comprising a portable communication unit comprising means for outputting an identifying signal, a computer terminal adapted to receive the identifying signal, and allow access to one or more processes run or operable by the computer terminal if the identifying signal received corresponds to one or more predefined identities, wherein the portable communication unit comprises a user operable element and is adapted to output the identifying signal only when or after the user operable element is operated by a user. The communication unit may be an RFID element adapted to be bent or tapped on in order for it to output the signal.

WO 2011/157750 A2

A COMPUTER ASSEMBLY COMPRISING A COMPUTER OPERABLE ONLY WHEN RECEIVING A SIGNAL FROM AN OPERABLE, PORTABLE UNIT

The present invention relates to a computer assembly comprising a computer or terminal and a portable unit which, when in the vicinity of the computer, renders the computer operable. In particular, the invention relates to an improvement in which the portable unit is user operable and only outputs the identity signal when operated by a user.

Systems are known from e.g. US2006/0294388, US 7,108,177 and US 7,287,693 which relate to the use of a portable RFID badge for identifying a user and his proximity to a computer to identify himself to the computer and render it operable. However, situations exist in which the user may, inspite of being in the vicinity of the computer, wish that the computer remains unoperable. Also, situations will exist in which a number of trusted or authorized users all are within the vicinity of the computer, which could confuse the system, if all requested access or log-on at the same time. The invention relates to a solution to that problem.

In a first aspect, the invention relates to a computer assembly comprising:

- a portable communication unit comprising means for outputting an identifying signal,
- a computer terminal adapted to:
    - receive the identifying signal, and
    - allow access to one or more processes run or operable by the computer terminal if the identifying signal received corresponds to one or more predefined identities,

wherein the portable communication unit comprises a user operable element and is adapted to output the identifying signal only when or after the user operable element is operated by a user.

In the present context, a computer assembly is an assembly comprising a number of interacting and/or communicating units. One of these units is a computer terminal, which may be a personal computer (PC), a server, a terminal, a PDA, a cell phone, a palm top computer, a lap top computer or the like. This terminal is able to run one or more processes giving the user access to one or more services thereon. Such processes may be word

processing, spread sheets, internet surfing, playing games, database access, correspondence/communication (mail, chat, voice, video or combinations thereof), data exchange/input/storing/output, printing, video/voice capture or playing/rendering or the like. In many situations, a user will gain access to a computer only if authorized to do so, usually by having a user name and a password to which the terminal is set up to accept. Different users may have different credentials and access to different types of processes or data on a terminal. This is controlled by the operating system and known means of defining user credentials and authorizations and enforcing these.

Another element of the assembly is a portable communication unit. In this respect, portable will mean that the unit is no larger than a laptop computer. Usually, portable elements with rather simple functionality and especially not requiring a large monitor or display will be the size and weight of a cellphone or smaller. Presently, the unit may be as small as a badge, credit card or tag, as are known for identification badges/tags for access control using e.g. RFID communication.

The portable communication unit comprises means for outputting an identifying signal. These means usually will be an antenna or the like, depending on the actual form of the signal. Preferably, the signal is transmitted in a wireless manner, such as using radio waves, Bluetooth®, WLAN, RFID, optical wavelengths, or the like. Thus, the outputting means may be an antenna, a light emitting diode, laser, or the like.

The signal, being an identifying signal, preferably has therein information particular to the actual user or a group to which the user belongs and/or an ID of the portable communication unit. Usually, the assembly will comprise one or more terminals and a plurality of portable units, where different units will output identifying signals which are different in order for the terminal(s) to be able to differ between users or units.

The terminal is adapted to receive the signal and thus preferably comprises a receiving means, such as an antenna, if the signal is transmitted in a wireless manner using e.g. radio waves, or a radiation detector, if the signal is transmitted as radiation.

It is noted that the receiving means need not be a fixed part of the terminal, as long as the terminal is able to receive the information from the receiving means. In one situation, a single receiving means is positioned in a room with multiple terminals, where all terminals, or all terminals not presently in use, may be available to the user. In a number of embodiments, however, it is desired that each terminal has or is connected to its "own" receiving means.

Having received the identifying signal, the computer may use this as a standard log-on procedure and thus allow the user access in the same manner as if the user had usual username and password to the terminal. Thus, the processes actually running (which may be communication with databases, the internet or the like) and processes which may be initiated if not run (which could be database access, mail programs, spreadsheets, chat forums or the like) may be made available to the user in the standard manner. As usual, the user may gain access to the present state of his latest session on the terminal or any other terminal, which could be the situation where the terminals are operated via a central server, or a "fresh" session may start.

Thus, as is the situation when a user logs-on using username and password, information in the identifying signal may be compared to a list of authorized users or information identifying these, and allowability of the log-on may be determined from this comparison.

According to the invention, the portable communication unit comprises a user operable element and is adapted to output the identifying signal only when or after the user operable element is operated by a user. In this connection, a user operable element may be any type of element which, after engagement or operation of a user will output a signal or alter a mode which is determinable by other elements. Thus, a user operable element may be a switch, a contact, a push button, a deformation sensor, such as for sensing bending, twisting, stretching, or the like using e.g. a strain gauge, a piezo element or the like.

Then, the identifying signal may be output as a consequence of the operation of the operation of the user operable element or may be output within a predetermined period of time thereafter but controlled by another action, such as the receipt of an interrogating signal from the terminal. In the latter situation, the unit may await the other action for a predetermined period of time after operation of the operable element, and then output the signal.

In one embodiment, the outputting means are adapted to output the identifying signal along a predetermined direction in relation to a main surface of the portable communication unit. Especially interesting is an embodiment wherein the outputting means are adapted to output the signal along a narrow beam along the direction. In this context, a narrow beam is a beam having a FWHM angle of up to 10 degrees from a centre line, such as up to 5 degrees from the centre line (both sides of the centre line).

In this manner, it is prevented that multiple terminals present within reach of the identifying signal may allow access to the processes at the same time. In this manner, the unit may be directed toward a selected terminal so that only this terminal receives the identifying signal.

Usual means for directing a signal along a direction and in a more or less narrow beam are lenses for optical communication and so-called directors for electromagnetic communication. Directors may be conducting elements positioned in relation to the antenna to shape the field output. One situation may be a tag or badge worn on the chest of a person primarily outputting the signal perpendicularly to its surface and thus in a direction in front of the person.

In a preferred embodiment, the outputting means is an RFID transducer. This is a well proven technology which is cheap, rugged and versatile.

Another manner of preventing accidental log-on by unauthorized persons is one wherein the outputting means are adapted to output the identifying signal so as to be detectable only within a predetermined distance, such no more than 3m, preferably no more than 2m, such as no more than l m or even no more than V2m, from the portable communication unit. Usually, this is obtained by ensuring that the signal is output with a signal strength within a desired interval or with a maximum strength which is pre-defined.

If further security is desired so that only authorized persons are allowed access to the processes on the terminal, the user operable element may adapted to derive biometric data from a user and compare the derived data to predefined data corresponding to one or more predefined identities and output the identifying signal only if the comparison indicates a match between the identity of the user and one of the one or more identities. Alternatively, the portable communication unit may derive such data and forward these to the terminal as or with the Identifying signal. In this situation, biometric data may be fingerprints, iris detection, voice recognition, or the like.

In a preferred manner, the user operable element is adapted to output a signal when a predetermined force is exerted thereto by the user. Thus, if the force is lower than the predetermined force, no activation is seen. This may prevent accidental activation of the unit.

Naturally, it may additionally or alternatively be required that the user performs a number of force exertions, such as in a given pattern or a given rhythm, for the unit to output the signal.

The most preferred user operable element comprises a piezo actuator. This very rugged and simple actuator will output a signal when deformed, such as bent or simply tapped on. The above minimum force required may be set as a minimum output of the piezo actuator.

Naturally, logging-of of the terminal or terminating access to the processes may also be of interest, if or when the user is no longer interested in using the terminal. In this respect, the computer terminal may be adapted to constantly or intermittently output an inquiry signal and the portable unit is adapted to receive the inquiry signal and output the identifying signal, if an identifying signal has been output within a first period of time, where the computer terminal then is adapted to deny access to the one or more processes, if no identifying signal has been received after a second period of time. Thus, a communication takes place between the terminal and the unit, after the unit has been "activated", as long as the communication is able to commence. The inquiry signal may be output only when communicating with the unit or may be output at all times.

Depending on the desired security, the terminal may output the enquiry signal every second, every minute, every 5 minutes, every 15 minutes, and any frequency there between.

The unit can be adapted to respond to the inquiry signal by outputting the identifying signal - or another signal - as long as the inquiry signal is received within a predetermined period of time, such as 15, 14, 13, 12, 11, 10, 9, 8, 7, 6, 5, 4, 3 or 2 minutes, 1 minute or even less. If the inquiry signal is output periodically, the first period of time usually will be selected longer than this period, so that communication continues. If the inquiry signal is output continuously, the identifying signal may be output when desired.

The terminal is adapted to monitor the receipt of the identifying signal in order to ensure that the unit is in the vicinity of the terminal or at least that the user is still interested in access to the terminal. If no identifying signal has been received within the second period of time, the terminal will assume that the unit is no longer within communication range and thus deny access to the processes and e.g. log-of the user. The second period of time will preferably be selected sufficiently long to ensure that an identifying signal output from a unit in the vicinity is allowed to be transmitted, so that unintended log-of is prevented.

Another manner of logging-of or denying access to the processes is one wherein:

- the portable unit is adapted to, upon another operation by the user of the user operable element, output a cancelling signal,

- the computer terminal is adapted to receive the cancelling signal and subsequently deny access to the one or more processes.

The two logging-of methods may be combined to obtain the possibility of logging-of while being in the vicinity of the terminal and still have the certainty that logging-of will under all circumstances automatically take place when leaving the vicinity of the terminal.

Thus, even though the unit is in communicating distance with the terminal, and possibly communicating using the above-mentioned exchange of inquiry signals and acknowledgement signals or identification signals from the unit, the user may log-of the terminal or deny access to the processes by operating the user operable element and thereby causing the outputting of the cancelling signal.

Usually, the cancelling signal will be different from the identifying signal but will preferably comprise information identifying the user in order to prevent unintended log-of of other users on other terminals.

The operation of the user operable element may be the same operation, which is possible when the unit is aware that it is still logged-on. This could be the situation where the unit and terminal have been communicating while the user has had access to the terminal.

Alternatively, the operation may be another operation, such as an operation of another user operable element or another operation of the same user operable element. This other operation may be multiple operations (tappings, bendings, deformations, force exertions) allowing the unit to differ between an operation indicating a desire to gain access to the processes and an operation indicating a desire to no longer gain that access.

A second aspect of the invention relates to a portable communication unit for use in the assembly according to the first aspect of the invention. It is noted that this unit can have some of or all of the above-mentioned features and abilities.

A third aspect of the invention relates to a method of operating a computer assembly comprising a portable communication unit and a computer terminal, the method comprising the steps of:

- the portable communication unit outputting an identifying signal, and

- the computer terminal receiving the identifying signal, and allowing access to one or more processes run or operable by the computer terminal if the identifying signal received corresponds to one or more predefined identities,

wherein the outputting step comprises a user operating an operable element of the portable communication unit which outputs the identifying signal only when or after the user operable element is operated by the user.

In a first embodiment, the outputting step comprises outputting the identifying signal along a predetermined direction in relation to a main surface of the portable communication unit. Preferably, the outputting means are adapted to output the signal along a narrow beam along the direction. As described above, this direction and the narrowness of the beam may be controlled or defined by known elements.

In a preferred embodiment, the outputting step comprises outputting the identifying signal as an RF signal.

In another preferred embodiment, the outputting step comprises outputting the identifying signal so as to be detectable only within a predetermined distance from the portable communication unit. In one situation, this is obtained by controlling a signal strength to be below a predetermined maximum strength or within a predetermined interval. Suitable distances are described above.

In a particular embodiment, the outputting step comprises deriving biometric data from a user, comparing the derived data to predefined data corresponding to one or more predefined identities and outputting the identifying signal only if the comparison indicates a match between the identity of the user and one of the one or more identities.

In a preferred embodiment, the outputting step comprises the portable unit outputting the identifying signal when a predetermined force is exerted thereto by the user. A particularly desired embodiment is one wherein the user operable element comprises a piezo actuator, where the user operating step comprises the piezo actuator outputting a signal when deformed by a force exerted by the user. As mentioned above, the deformation may be a bending of or tapping on the unit. Also, the user may be required to perform multiple force exertions, such as a predetermined number or in a predetermined rhythm, before the identifying signal is output.

Logging-of is also desired in most instances. Thus, the method may further comprise the steps of:

- the computer terminal constantly or periodically/intermittently outputting an inquiry signal and

- the portable unit receiving the inquiry signal and outputting the identifying signal, if a former identifying signal has been output within a first period of time,

the computer terminal denying access to the one or more processes, if no identifying signal has been received after a second period of time.

In this respect, periodic/intermittent outputting of the inquiry signal may be a periodic or quasi-periodic outputting of the signal. A constant outputting of the signal may be a situation where the signal simply is a given frequency to which the unit responds.

In order to prevent unintended logging-out, the first period of time should be selected longer than any period or longest period of the inquiring signal if periodic/intermittent. If the inquiring signal is continuous or constantly output, the first period of time may be selected more freely. Suitable periods of time are described above.

The second period of time should be selected so as to have time to receive a signal from the unit if in communicating range and communicating.

Another manner of logging-of is one comprising the steps of:

- the portable unit, upon another operation by the user of the user operable element, outputting a cancelling signal,

- the computer terminal receiving the cancelling signal and subsequently denying access to the one or more processes.

As mentioned above, the two logging-of methods may be combined.

Also, the cancelling signal usually will be different from the identifying signal but will also comprise information relating to the identity of the user, and the operation may be the same operation or another operation of the user operable element.

A fourth aspect of the invention relates to a method of operating a portable communication unit according to the second aspect of the invention, the method comprising the steps of:

- a user operating the operable element and

- the portable communication unit outputting an identifying signal only when or after the user operable element is operated by the user.

In one embodiment, the outputting step comprises outputting the identifying signal along a predetermined direction in relation to a main surface of the portable communication unit. Preferably, the outputting means are adapted to output the signal along a narrow beam along the direction.

In another embodiment, the outputting step comprises outputting the identifying signal as an RF signal.

In yet another embodiment, the outputting step comprises outputting the identifying signal so as to be detectable only within a predetermined distance from the portable communication unit.

In a more safety focused embodiment, the outputting step comprises deriving biometric data from a user, comparing the derived data to predefined data corresponding to one or more predefined identities and outputting the identifying signal only if the comparison indicates a match between the identity of the user and one of the one or more identities.

In a preferred embodiment, the outputting step comprises outputting the identifying signal when a predetermined force is exerted thereto by the user. Preferably, the user operable element comprises a piezo actuator, where the user operating step comprises the piezo actuator outputting a signal when deformed by a force exerted by the user. As mentioned, the user may be required to perform multiple deformations, such as a predetermined number or in a predetermined rhythm.

An interesting embodiment further comprises the steps of:

- receiving a constantly or periodically/intermittently transmitted inquiry signal and

- outputting the identifying signal, if an earlier identifying signal has been output within a first period of time.

That or another embodiment may further comprise the steps of:

- outputting, upon another operation by the user of the user operable element, outputting a cancelling signal being different from the identifying signal.

In the following, preferred embodiments will be described with reference to the drawings, wherein

Fig. 1 is a schematic diagram of a system incorporating features in accordance with an exemplary embodiment of the present invention;

Fig. 2 illustrates one embodiment of a digital verification process of an RFID tag with a remote reader/transceiver of the system in Fig. 1;

Fig. 3 represents one embodiment of an RFID tag public key validation process;

Fig. 4 is a flow chart schematically illustrating a method of operation of the system;

Fig. 5 is a flow chart schematically illustrating another method of operation of the system;

Fig. 6 shows a number of exemplary devices incorporating an RFID tag of the system; and

Fig. 7 illustrates a portable unit for use according to the invention

The major parts of the following description have been derived from US7,108,177 which, however, uses a standard portable RFID element which automatically will respond to any inquiring signal from a transceiver, where the portable unit according to the invention will not do so without having been operated by the user.

As seen in Fig. 1, the user identification system 10 secures access to a resource system of a ressource A. In this embodiment, the resource A, which is secured and to which a user seeks access is schematically represented as a computer terminal or work station A10. The work terminal A10 is a representative station, and is shown as a single station for example purposes only. Station A10 may be a stand alone PC connected to the user identification system as will be described below, or may be any desired number of terminals or devices connected to the system 10. Further, resource A may be communicably connected to other devices/terminals either by a LAN or other desired network (not shown) so that access to resource A serves as a portal to the other devices communicating with resource A, but not independently secured by system 10. In alternate embodiments, resource A may be any other desired system or device to which access is secured by system 10, such as private,

commercial or public facility, conveyances and facilities transportation and shipping systems, or any other suitable system to which secure access is desired. In still other alternate embodiments the system 10 may secure any desired number of individual resources which may be of the same or of different types.

Still referring to Fig. 1, the user identification system 10 employs RFID technology to effect a secure way of providing user identity to terminal A when the user is in a predetermined proximity to the terminal and operates the RFID tag 100, as will be described further below. The user identification system 10 generally comprises a host server 12 and transceiver 14 for communicating with an RFID tag 100 in the possession of the user. In the embodiment shown in Fig. 1, a representative host server 12, transceiver 14 and RFID tag 100 are shown for example purposes, and system 10 may comprise any desired number of host processors, transceivers and RFID tags. In general, the RFID tag 100 holds user unique data or user credentials (i.e. capable of establishing the identity of the user tag holder) that are communicated via transceiver 14 to the host processor 12 upon arrival of the user within a predetermined distance of terminal or station A and upon activation of the RFID tag 100. The host server 12 determines the identity and hence access authorization of the tag holder from the user credentials, and automatically enables access (i.e. "logs on" the tag holder) into terminal A. Departure of the user (and hence the RFID tag) from the proximity of the terminal A, may be automatically signaled via transceiver 14 to host server 12 which automatically initiates access termination (i.e. "log-off") to terminal A. Alternatively, another activation of the RFID tag 100 may signal to the terminal that access termination is desired. Hence, system 10 performs user identification and potentially also access initiation/termination ("log-on/log-off") upon instructions from the tag holder.

Host server 12 may be any suitable computer station. Shown representatively in Fig. 1 as a single station, host server 12 may comprise any desired number of process stations. Host server 12 may be part of terminal A. Transceiver 14 may also be part of terminal A if desired. The multiprocess stations of host server 12 may be communicably connected by any suitable communication linking means such as a LAN, Internet or wireless communication links. As seen in Fig. 1, the host server 12 may include a suitable processor 20 and memory 22 with programming for an operating system. Memory 22 may include memory registers capable of storing a database 22a containing electronic data embodying the unique user credentials used in establishing the user identity. The user credentials, which as noted before are unique for each user, may be of any suitable kind, such as a character string, and may be arranged in any suitable manner to serve user identification with the desired level of security. For example, the user credentials may be structured in a manner somewhat similar to the "log-on" identifiers and "password" form of conventional log-on systems. In this case each RFID Tag (to be described in greater detail below) may have a unique tag identifier (relating the

tag among a population of tags as well as to a particular user) and predetermined user unique identification data. The unique tag identifier also aids authentication as will be seen below. The predetermined user unique identification data may be any desirable electronically communicable data assigned uniquely to a user. The predetermined tag unique identification data may also be any desirable electronically communicable data assigned uniquely to the tag. As will be described further below, the tag identifier and user identifier may be established at any desired time such as at the time the RFID tag is assigned to the user. The unique tag identifier and unique user identifier may serve as the unique user credentials. In alternate embodiments, the user unique credentials may have any other suitable form. The database 22a in the memory registers 22 of the host server may have any suitable architecture arranged to be interfaced with or accessed by any desirable access protocol. For example, the database 22a may be arranged generally in accordance with the lightweight directory access protocol (LDAP). Though in alternate embodiments the database may be structured in accordance with any other suitable arrangement and access protocol.

In the embodiment where database 22a has a general LDAP arrangement, the database may have a hierarchical type data store distribution. By way of example, each of the resources (similar to resource A) served by the host server 12 may have a segregated and independently addressed storage location holding data stores with user identification information for that resource. Thus, the data stores with user credentials for resource A may be located in a storage location having an address or identifier associated with resource A. Further organizational distribution may be provided (such as at a sub-resource or sub-location level if desired). In this embodiment, user credential data may be held in a separate data store of a corresponding location. This allows the database 22a in host server 12 to efficiently store user identification information related to any desired number of different resources (similar to resource A) and facilitate ready access to any desired data stores related to a desired resource.

As may be realized, the address information assigned to each data store in the database, and enabling the interface program in host server 12 to access the data stores, reflects the distribution/architecture of the database. As seen in Fig. 1, the host server 12 may have a software suite 24 for interfacing with and accessing/reading information stored in data stores of database 22a. Software suite 24 may also be capable of writing or storing data into data stores of the database, and if desired of designating memory space in memory 22 as data stores for database 22a. Further, software suite 24 may include suitable communication software to interface with and operate transceivers (similar to transceiver 14) for effecting bidirectional communications with RFID tags such as tag 100. Further still, software suite 24 is capable of communicating with the resources it serves, such as resource A, to enable user access/"log-on" (i.e. to provide the resource user with the roles and privileges associated

with log-on) to the resources, and to remove access/"log-off" the user as will be described further below.

Still referring to Fig. 1, there is shown an operation area 18 including the station AlO of resource A, and transceiver 14. Area 18 schematically represents the geographic region where a RFID tag 100 held by a user desiring access to resource A is capable of communicating with transceiver 14. The boundaries of area 18 may be established as desired, and the communication range of the transceiver 14 may be set accordingly. By way of example, the operation area 18 may be established to be within the immediate proximity (about ½-l m) of the station AlO. The location, relative to station AlO, and communication range of the transceiver 14 are thus appropriately defined. Log-on and log-off of a user onto resource station A10, as will be described in greater detail below, occurs respectively when the RFID tag 100 held by the user (and with the appropriate user credentials thereon) is correspondingly brought into or removed from the aforementioned proximate boundaries of the operation area 18 and operated around that time. In one embodiment, the size or bounds of the operation area may be established as large as desired, and may be capable of encompassing any desired number of users. In other embodiments, the operation area 18 may include more than one station (similar to station A10) for more than one resource (similar to resource A), and may also include more than one transceiver (similar to transceiver 14). For example, the operation area may be a room (not shown) in a facility (or possibly the entire facility or any portion thereof) holding multiple stations (similar to station A10) of multiple resources. Multiple users may be located in the operation area, and some users may be entitled to access some but not all the resource stations in the operation area. As seen in Fig. 1, host server 12 may be connected to serve any desired number of other operation areas 18A (only the area 18 is shown for example purposes) that are similar to area 18. As may be realized, resource A may have secured stations (similar to station A10) in the other operation areas 18A served by server 12 of system 10. In this embodiment, the resource station A10, in area 18, and other resource stations (similar to station A10) in other areas 18A may be provided with an identifier related to the area 18, 18A in which the station is situated. Hence, multiple resource stations sharing an operation area may have a common identifier. The identifier, which may be communicated to server 12 upon connection to a given resource station, may be used to independently address desired resource stations in desired operation areas 18, 18A. Each of the operation areas 18, 18A may be connected to the server 12 via a communication system 16 such as the internet or modems. Alternatively, if a user wishes to use one of a plurality of stations to which the user is authorized, but some of which are in use, an available terminal receiving the signal from the users RFID tag 100 may avail itself to the user by e.g. logging-on on behalf of the user and e.g. flashing its screen.

As noted before, each operation area 18, 18A of system 10 has one or more transceivers, similar to transceiver 14. The transceiver(s) generally comprises suitable circuitry (not shown) and an antenna 14a capable of bi-directional communication or coupling, according to a desired communication protocol, with RFID tag 100 when the tag is within the operation area 18, 18A. As may be realized, the transceiver 14 is also capable of converting the response signal from the RFID tag to suitable electronic format for communication to server 12. As noted before, the communication range of the transceiver 14 is established to define the desired size of the operation area 18, 18A. Transceiver 14 may be capable of coupling with one or more of the RFID tags 100 in the operation area 18, 18A. To facilitate coupling with multiple RFID tags (similar to tag 100), the transceiver 14, and/or the server 12 controlling operation of the transceiver, may include a multiple RFID anti-collision interrogation system (not shown) a suitable example of which is disclosed in U.S. patent application Ser. No. 10/740,983, filed Dec. 19, 2003, and incorporated by reference herein in its entirety. In this embodiment, the transceiver may be provided with an identifier 14b that for example, may be stored in a suitable memory (not shown) of the transceiver. The transceiver identifier 14b, similar to the resource station identifier disclosed before, relates the transceiver 14 to the operation area 18 in which the transceiver is operating. The transceiver identifier 14b may be stored or otherwise entered at any desired time such as at system setup or upon connection of the transceiver to the server. The transceiver identifier 14b, may be communicated at any desired time, such as when communicating the response signal received from the RFID tag, to the server. Hence, the transceiver identifier 14b may be used by the server 12 to associate the particular transceiver 14 to the corresponding resource station A10, and the RFID tag(s) 100 (and thus the users) communicating with the given transceiver with the corresponding resource station A10. This allows the server 12, upon verification of the user credentials from the RFID communication received via transceiver 14, to selectively send a command to the corresponding resource station A10 to enable user access/log-on. Conversely, upon receipt of a suitable signal from the transceiver 14 that the RFID tag is no longer present in the operating area 18, the server 12 may selectively transmit a command to the corresponding resource station A10 to log-off/close access to the departed user. In this manner, server 12 selectively controls access to desired stations of a given resource without providing access to resource stations where access is not desired.

Fig. 1 shows an RFID tag 100 used for access to the resource stations A10 of resource A. Tag 100 shown in Fig. 1 is a representative tag, and any number of tags similar to RFID tag 100, each as noted before with unique user credentials, may be issued or otherwise available for use to log-on/log-off stations of resource A. In this embodiment, RFID tag 100 may be specifically related to resource A (i.e. tag 100 serves to provide access specifically to resource A). RFID tag 100 may also be specifically related to other resources (not shown)

having stations located in common with resource station A10 in operation area 18, or independently located. As seen in Fig. 1, tag 100 has suitable RFID circuitry 102 to receive RF interrogation communication 200 from transceiver 14 and transmit a suitable RF response communication 202 to the transceiver. In the exemplary embodiment, the RFID circuitry 102 may be "active" (i.e. capable of actively generating the RF response communication 202, rather than modulating the reflected interrogation signal).

Accordingly, tag 100 may include a battery 110 or other suitable power supply (e.g. protocol) connected and supplying power to the RFID circuitry 102 being formed by a coil 102' and a processing unit 103. In alternate embodiments the RFID circuitry of the tag may be "passive" or "active/passive". Tag 100 also has suitable memory 104, such as ROM or EPROM memory, with registers 108 for storing for example the unique tag identification data 108a, and unique user identification data 108b. Memory 104 in this embodiment includes suitable encryption programming 106 to provide secure communication to transceiver 14/server 12. The software suite 24 of the server 12 has suitable decryption capable of reading the data in the encrypted communication from the RFID tag.

Figure 7 illustrates two embodiments of the RFID tag 100. The tag 100 comprises, a coil 102' which, together with a processing unit 103, forms the RFID circuitry 102 and thus is able to receive the communication 200 and output the response 202. The unit 103 furthermore comprises memory 104, data 108a, etc. In addition, the tag 100 comprises a user operable element 113, which is adapted to output a signal when operated by the user. This element 113 may be powered by the battery 110 if desired so as to forward power to the unit 103 when operated - or break a power supply if desired. Alternatively, the element 113 may be a switch or the like opening or closing a circuit upon manipulation.

A preferred type of element 113 is a piezo element which has the advantage of itself providing a voltage when deformed, such as by bending or tapping on the tag 100. Piezo elements have the advantage of being rugged and very simple and thus hard to break. This type of element 113 need then not be connected to the battery 110.

The operation of the unit 103 may be as that described above and below and thus that of receiving the interrogation communication 200 and outputting the response 202 when possible. A switch 114 is, however, provided which prevents communication from the unit 103 to the coil 102', unless instructed otherwise by the unit 103 - or alternatively the element 113. Thus, when the switch 114 is open, no interrogation communication 200 is forwarded to the element 103, and no responses 202 are output. When the switch 114 is closed, interrogation and response is handled as described above.

An alternative is one where the switch 114 is omitted and the unit 103 is adapted to output the signal only when the element 113 has been operated and fed a signal to the unit 103

The lower part of figure 7 illustrates a passive tag 100 which does not have a battery 110. In this embodiment, the element 113 may itself operate or control the switch 114. In one situation, the switch 114 comprises a FET adapted to open or close the connection between the coil 102' and unit 103, which FET is powered by power provided by the switch 113, which may be a piezo element and potentially a capacitor or charge pump for storing the power received from the piezo element and thus maintain the FET open, and thus the coil 102' operable, for a period of time.

Alternatively, the element 113 needs not be in the signal path from the unit 103 to the switch 114 or coil 102'. The element 113 may feed a signal directly to the unit 103 outside of the signal path from unit 103 to coil 102'.

Having operated the element 113 and thus allowed or facilitated outputting of the response communication 202, the station A10 now logs on and allows the identified user access to the processes etc. thereon. In this situation, logging-of is also of interest.

In this respect, it may be desired to have the station A10 stay logged on until receiving a signal from the tag 100 to log-of. Alternatively, the station A10 may log-of when the tag 100 is no longer in the vicinity thereof. A combination of the two may be the optimum solution.

As to the first solution, the unit 103 of the tag 100 will then be able to output a log-of signal when the element 113 is operated. In this situation, the tag 100 preferably is aware of it being logged on, which could be the situation if constant or intermittent communication takes place between the station A10 and the tag 100 while being logged on. In this situation, the station A10 may constantly or intermittently output interrogation communication 200. The tag 100, once the element 113 is operated and the tag 100 has output the response communication 202, may remain "open" for a longer period of time than the period of any intermittent communication of the station A10. Therefore, the tag 100 will receive the next communication 200 and output the communication 202 and thus reset the timing to the next expected communication 200. This constant communication will continue until stopped, which may be the situation if the user operates the element 113 again. In this situation, a log-of signal may be output in accordance to which the station A10 acts. Also, subsequently, the switch 114 may open, whereby no further communication will take place.

Alternatively, the communication may continue until no interrogation communication 200 is received, which would be the situation, if the tag 100 is moved too far from the station A10.

Thus, in that situation, the station A10 would then not receive a response communication 202 and thus log-of, and the tag 100 would stop communication, as it does not receive communication 200, and thus open switch 114.

Naturally, switch 114 is not required. The unit 103 may itself be operable to allow or prevent/refuse communication via the coil 102', depending on the operation of the element 113.

Also, in more extreme cases, the element 113 may not be operable by just any person in that it may comprise a sensor or other instrument for deriving biometric data (blood sample, iris detection, fingerprint, voice recognition or the like) from the user and only output the signal required when the biometric data match those of the authorized user.

Alternatively, the element 113 may derive the biometric data and forward these to the station A10 in order for the station A10 to determine whether to allow this person access or not.

The communication between RFID tag 100 and server 12 may be secured by public/private key cryptography. By way of example, the tag memory 104 may have stored therein a tag private key. Further, to facilitate an authentication function of the tag 100, memory 104 of the tag 100 in this embodiment may hold a tag provider or tag vendor private key. As may be realized, tags similar to tag 100 are issued or provided to users of resource A by one or more providers. The tag provider has a private key that is registered in the tag memory 104 at any time before or during issue of the tag to the user. The tag provider also has a public key that is stored in the memory of 22 of server 12. The tag private key, is unique to the tag 100 and hence may form part of the unique tag identifier of the tag 100. The matching tag public key to the tag private key is also stored in the memory 22 of server 12. The tag private key may also be registered in tag memory 104 at any time before or during issue of the tag to the user. User unique identification data 108b may be registered in the tag memory 104 when the tag provider issues the tag 100 to the user. As noted before, the user unique identification data are also provided by any suitable secure means to the server 12 and are stored in the suitable data store for the appropriate resource in database 22a.

The tag 100 may use the tag private key to sign data transmitted in the response 202 to the interrogation command 201 from transceiver 14. Fig. 2 illustrates one embodiment of a validation process for data signatures of RFID tag 100. The tag data elements, such as for example tag identification data 108a (see also Fig. 1) 502 are applied to a hash function 504 to result in a hash value 505. Hash function 504 may be stored in RFID tag memory 104. The hash value 505 and the tag private key 508 (from memory 106) are combined to produce the

signature function 506. Signature function 506 is transmitted to transceiver 14 in communication response 702 along with tag data elements 502. During verification performed by the server 12, the hash value 512, produced from the hash function 510 as applied to the tag data elements 502, is inputted to the tag data signature verifier 514, of the server 12 together with the received signature and the tag public key 516 from server memory. The result 518 determines the validity or invalidity of the tag data elements 502 after transmission. Authentication of the tag 100 is schematically illustrated in Fig. 3. In this embodiment, the tag data elements in the tag response transmission 202, and the tag public key 602 are hashed via a hash function 604 to produce a hash value 605. The hash value 605 and vendor public key 608 are used to produce the signature function 606 transmitted to the server via transceiver 14. The vendor private key 616 from the server memory is used together with the received signature function key 606 and hash value 612 in the tag public key signature verifier 614 to determine if the tag data elements are associated with the proper authority and are determined to be valid or invalid 618. Authentication of the tag and validation of the RFID tag data as described above assures that the message incorporated in the communication from the tag 100 is as transmitted from the tag 100. The response communication 202 may also contain the user unique identification data encrypted utilizing standard public key encryption techniques. The user identification data is related to the server 12, upon receipt by the transceiver 14, and decrypted by the server. The response communication may further contain data identifying the resource A to which tag 100 is related as noted above. This data may serve or be formatted to provide the directory, and/or subdirectory, address in server database 22a holding the data store with the user identification credentials for tag 100. After reception of the user credentials transmitted by tag 100, server 12 performs a comparison of the received user credentials with corresponding stored user credentials from the database. Upon finding a match between received and stored user credentials, server 12 as noted before sends a writable enable access command to the resource station A10 in the appropriate operation area 18, thereby effecting user "log-on" the resource station. The server 12 may also inform the resource A or resource station of the identity of the user being logged on by for example sending the resource station A10 a data entry (e.g. password) enabling the resource A to identify the user/tag holder.

Fig. 4, schematically illustrates a suitable process for effecting automatic "log-on" of a user onto resource station A10 upon receipt of the transmission 202. As seen in Fig. 1, the "log-on" process may commence when the user in possession of RFID tag 100 (as will be described below) enters the operation area 18 and operates the tag 100. Transceiver 14 may be capable of sensing when the RFID tag 100 becomes active inside the operation area.

As may be realized, locator signal range may be established so that the transceiver 14 will not receive tag locator signals when the tag 100 is located outside the operation area 18 or is not operated. In alternate embodiments the transceiver 14 may send the interrogation signal (similar to interrogation signal 200), continuously or with sufficient periodicity so that the RFID tag may be interrogated within a substantially imperceptible short duration after entrance into or activation in the operation area. In this case, reception of the response communication (similar to communication 202 in Fig. 1) from the RFID tag would inform the transceiver/server of the presence of the activated tag in the operation area.

Thus, the log-on process commences with the transceiver 14 transmitting the interrogation signal as illustrated in block LI of Fig. 4. If the tag 100 is activated by having been operated by the user, block LI', it responds to the transceiver interrogation, in block L2 the RFID tag 100 by sending a signed response communication 202 transmitting the encrypted unique tag identifier and user credentials from the tag memory as described before. If the tag is not activated, no signal is output, and log-on is denied (block L4).

The response communication, if received by the transceiver 14, is related to the server 12 for authentication of the public key and validation of the tag (see block L3 in Fig. 4). If the server determines that the signature is not authentic and/or the tag is invalid, the "log-on" process is stopped and resource access is not allowed, block L4. If in block L3, the server authenticates the public key and validates the tag, the log-on process continues as in block L5, with the server reading the user credentials received from the tag and comparing the received credentials with the user credentials in the appropriate directory in database 22a (see also Fig. 1) corresponding to resource A. If the server cannot match the received user credentials with those in the corresponding data store of database 22a, in block L6, the server stops the "log-in" process and access to the resource A is denied (block L4). If in block L6, the user credentials transmitted by the RFID tag are verified, then in block L7 the server sends a "log-on" command to the desired resource station A10 (identified for example by the transceiver identification) thereby logging-on the user. As noted before, the server may also communicate to the resource A, the identity (i.e. data representing the identity) of the user being logged on.

As the log-on, logging-of may be actively caused by the user by operating the station A10 accordingly or by activating the tag 100. The terminal, when logged on and receiving another transmission, may interpret this as a desire to log-of.

Fig. 5 schematically illustrates an alternative process by which the user is automatically logged off from the resource station A10. In block Ml of Fig. 5, the user is logged on the resource station A10, for example in the manner described above and illustrated in Fig. 4. In

this embodiment, however, the tag, once operated and within communication distance from the transceiver 14, will keep communicating with the transceiver, such as by maintaining outputting of the identification data, as long as it is within communication distance. Transceiver 14 may then be capable of sensing when the RFID tag 100 is no longer located in the operation area 18. For example, as noted before the RFID tag may send a periodic locator signal received by the transceiver 14 when the operated tag is in the operation area. Removal of the tag from operation area 18 causes the transceiver to stop receiving the periodic locator signal, which may be interpreted by the transceiver 14 to mean that the RFID tag 100 is no longer located in the operation area. In response the receiver 14 may send an interrogation signal to confirm presence or lack thereof. Also, the tag may then stop communicating until again activated. In alternate embodiments, the transceiver may send continuously or periodically an interrogation signal, similar to signal 200 in Fig. 1, to determine the presence of the activated RFID tag in the operation area. Failure to receive a response from the RFID tag 100 indicates that the tag is no longer present in the operation area. In any event, the "log-off" process is commenced automatically, and may be initiated by the transceiver sending an interrogation signal to confirm the presence or lack thereof of the tag 100 in the operation area, block M2 in Fig. 5. If the transceiver receives a response to the interrogation signal, block M3, then the "log-on" is maintained, block M4. If the transceiver receives no response from the tag in block M3, then the transceiver sends a suitable signal to the server indicating the tag 100 is no longer in the operation area 18. In block M4, the server, upon receiving such signal, may send a command to the appropriate resource station A10 to "log-off" the user.

The RFID tag 100 may be incorporated into any desired device or apparatus 300, 310, or 320 (see Fig. 6). By way of example and as shown in Fig. 6, the tag 100 may be included into a wristwatch 300, apparel 320, or card/badge 310. The RFID circuitry (similar to circuitry 102) may be applied to the device 300, 310, or 320 by any suitable means. For example, the RFID circuitry may be formed integral to the device or may be provided on a chip 100A that may be mechanically applied to the device. As may be realized, the devices 300 320 shown in Fig. 6 as having the RFID circuitry and operating as an RFID tag similar to tag 100 are merely exemplary, and in alternate embodiments the RFID tag may be encompassed into any suitable apparatus, device or object.

As described above, system 10 provides log-on and password entry into a resource such as a computer system when a user in possession of the invention's RFID transceiving mechanism is within the proximity of said resource and activates the tag.

The system 10 may effect automatic log-of of said user, should said user move outside the proximity boundary of the resource. The system provides users with an RFID tag 100

specifically key coded to said users unique credentials. The RFID transmitter is interfaced to the computing system 10, such that when an individual's RFID transceiver responds to the signal transmitted from the computer RFID transmitter, said individual's RFID (RFID tag) transceiver responds with a signal pattern uniquely describing said individual's unique credentials.

Further, the signal pattern sent from the individual's RFID Tag may be received by the system's transceiver, with said pattern being communicatively sent to the server of the system 10 which digitized said pattern to determine the identity of the user whose RFID tag produced the received pattern, when compared to information within the system 10.

The communications between the RFID tag and system's transmitter/receiver system may be encrypted and/or signed to provide security against eavesdroppers or third parties intent on compromising the security of the system. In this case, each RFID tag may have injected into it or have an application to generate a public/private key pair. Using Public Key Cryptographic and DiffieHellman session establishment methodologies, the RFID tag and associated computer system will be known and authenticated to each other.

It is noted that it could be desired to provide a more narrow communication signal 202 from the tag 100 in order to prevent the situation where the user is seated at one terminal 10A, activating the tag 100, and a user sitting at a neighbouring signal logging-on on another terminal on the basis of the communication 202 from the user. In the art, so-called directors or signal concentrators are known which cause the field output of the tag 100 to be more focused in one direction and thus weaker in other directions. Thus, a lower energy may be required to log-on using a director in this manner, as less energy is required to have the desired signal strength at a certain distance but within along the main direction of the signal.

CLAIMS

1. A computer assembly comprising:

- a portable communication unit comprising means for outputting an identifying signal,
- a computer terminal adapted to:
    - receive the identifying signal, and
    - allow access to one or more processes run or operable by the computer terminal if the identifying signal received corresponds to one or more predefined identities,

wherein the portable communication unit comprises a user operable element and is adapted to output the identifying signal only when or after the user operable element is operated by a user.

2. A computer assembly according to claim 1, wherein the outputting means are adapted to output the identifying signal along a predetermined direction in relation to a main surface of the portable communication unit.

3. A computer assembly according to claim 2, wherein the outputting means are adapted to output the signal along a narrow beam along the direction.

4. A computer assembly according to any of the preceding claims, wherein the outputting means is an RFID transducer.

5. A computer assembly according to any of the preceding claims, wherein the outputting means are adapted to output the identifying signal so as to be detectable only within a predetermined distance from the portable communication unit.

6. A computer assembly according to any of the preceding claims, wherein the user operable element is adapted to derive biometric data from a user and compare the derived data to predefined data corresponding to one or more predefined identities and output the identifying signal only if the comparison indicates a match between the identity of the user and one of the one or more identities.

7. A computer assembly according to any of the preceding claims, wherein the user operable element is adapted to output the signal when a predetermined force is exerted thereto by the user.

8. A computer assembly according to claim 7, wherein the user operable element comprises a piezo actuator.

9. A computer assembly according to any of the preceding claims wherein:

- the computer terminal is adapted to constantly or intermittently output an inquiry signal and

- the portable unit is adapted to receive the inquiry signal and output the identifying signal, if an identifying signal has been output within a first period of time,

the computer terminal being adapted to deny access to the one or more processes, if no identifying signal has been received after a second period of time.

10. A computer assembly according to any of the preceding claims, wherein:

- the portable unit is adapted to, upon another operation by the user of the user operable element, output a cancelling signal, and

- the computer terminal is adapted to receive the cancelling signal and subsequently deny access to the one or more processes.

11. A portable communication unit for use in the assembly according to any of the preceding claims.

12. A method of operating a computer assembly comprising a portable communication unit and a computer terminal, the method comprising the steps of:

- the portable communication unit outputting an identifying signal, and

- the computer terminal receiving the identifying signal, and allowing access to one or more processes run or operable by the computer terminal if the identifying signal received corresponds to one or more predefined identities,

wherein the outputting step comprises a user operating an operable element of the portable communication element which outputs the identifying signal only when or after the user operable element is operated by the user.

13. A method according to claim 12, wherein the outputting step comprises outputting the identifying signal along a predetermined direction in relation to a main surface of the portable communication unit.

14. A method according to claim 13, wherein the outputting means are adapted to output the signal along a narrow beam along the direction.

15. A method according to any of claims 12-14, wherein the outputting step comprises outputting the identifying signal as an RF signal.

16. A method according to any of claims 12-15, wherein the outputting step comprises outputting the identifying signal so as to be detectable only within a predetermined distance from the portable communication unit.

17. A method according to any of claims 12-16, wherein the outputting step comprises deriving biometric data from a user, comparing the derived data to predefined data corresponding to one or more predefined identities and outputting the identifying signal only if the comparison indicates a match between the identity of the user and one of the one or more identities.

18. A method according to any of claims 12-17, wherein the outputting step comprises the portable unit outputting the identifying signal when a predetermined force is exerted thereto by the user.

19. A method according to claim 18, wherein the user operable element comprises a piezo actuator, where the user operating step comprises the piezo actuator outputting a signal when deformed by a force exerted by the user.

20. A method according to any of claims 12-19 further comprising the steps of:

- the computer terminal constantly or periodically/intermittently outputting an inquiry signal and

- the portable unit receiving the inquiry signal and outputting the identifying signal, if an earlier identifying signal has been output within a first period of time,

the computer terminal denying access to the one or more processes, if no identifying signal has been received after a second period of time.

21. A method according to any of claims 12-20, further comprising the steps of:

- the portable unit, upon another operation by the user of the user operable element, outputting a cancelling signal,

- the computer terminal receiving the cancelling signal and subsequently denying access to the one or more processes.

22. A method of operating a portable communication unit according to claim 11, the method comprising the steps of:

- a user operating the operable element and

- the portable communication unit outputting an identifying signal only when or after the user operable element is operated by the user.

23. A method according to claim 22, wherein the outputting step comprises outputting the identifying signal along a predetermined direction in relation to a main surface of the portable communication unit.

24. A method according to claim 23, wherein the outputting means are adapted to output the signal along a narrow beam along the direction.

25. A method according to any of claims 22-24, wherein the outputting step comprises outputting the identifying signal as an RF signal.

26. A method according to any of claims 22-25, wherein the outputting step comprises outputting the identifying signal so as to be detectable only within a predetermined distance from the portable communication unit.

27. A method according to any of claims 22-26, wherein the outputting step comprises deriving biometric data from a user, comparing the derived data to predefined data

corresponding to one or more predefined identities and outputting the identifying signal only if the comparison indicates a match between the identity of the user and one of the one or more identities.

28. A method according to any of claims 22-27, wherein the outputting step comprises outputting the identifying signal when a predetermined force is exerted thereto by the user.

29. A method according to claim 28, wherein the user operable element comprises a piezo actuator, where the user operating step comprises the piezo actuator outputting a signal when deformed by a force exerted by the user.

30. A method according to any of claims 22-29 further comprising the steps of:

- receiving a constantly or periodically/intermittently transmitted inquiry signal and

- outputting the identifying signal, if a former identifying signal has been output within a first period of time

31. A method according to any of claims 21-30, further comprising the steps of:

- outputting, upon another operation by the user of the user operable element, outputting a cancelling signal being different from the identifying signal.

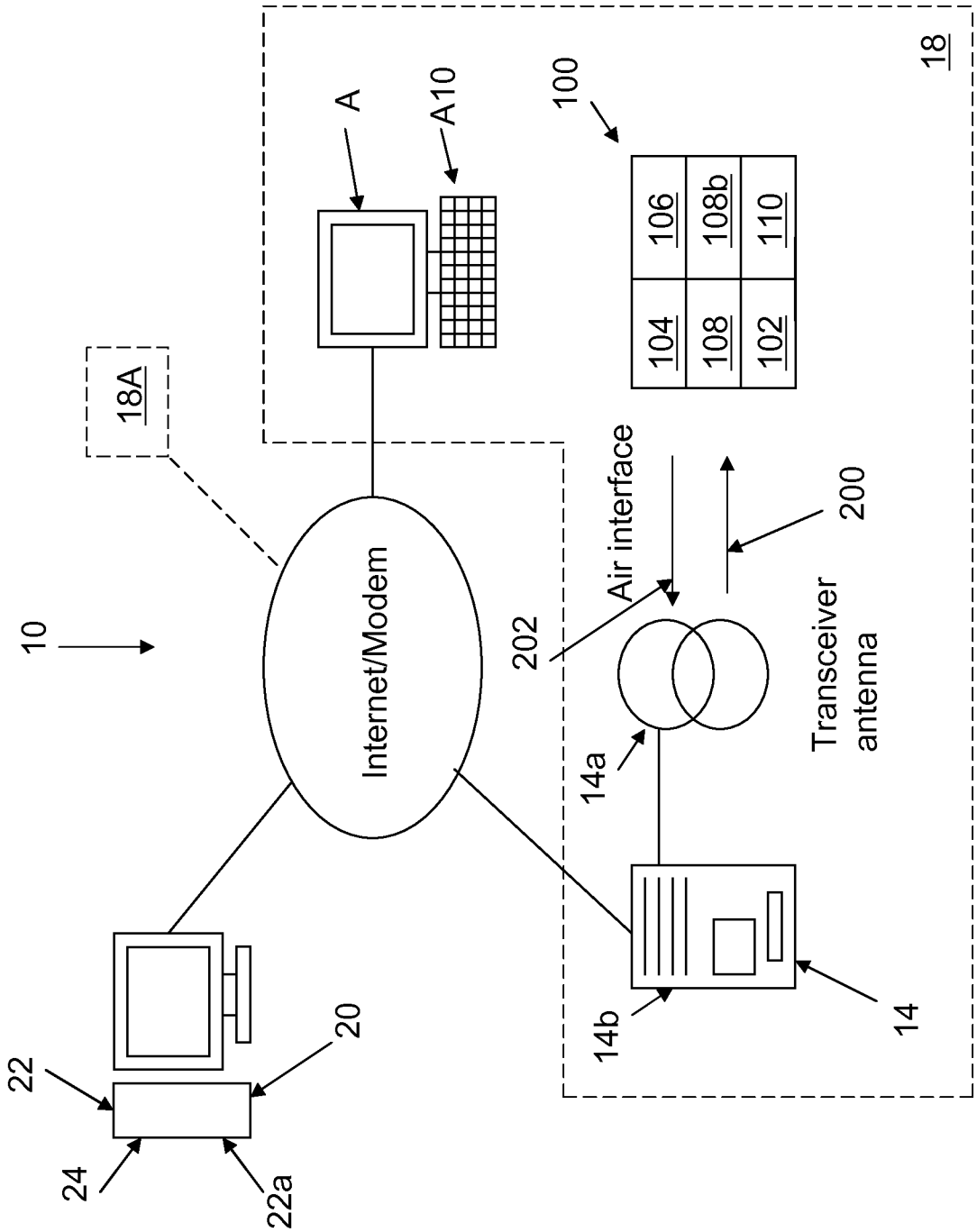

18
100
A
A10
106
108b
110
104
108
102
18A
10
Internet/Modem
202
Air interface
200
Transceiver antenna
14a
14b
14
20
22
24
22a

Figure 1

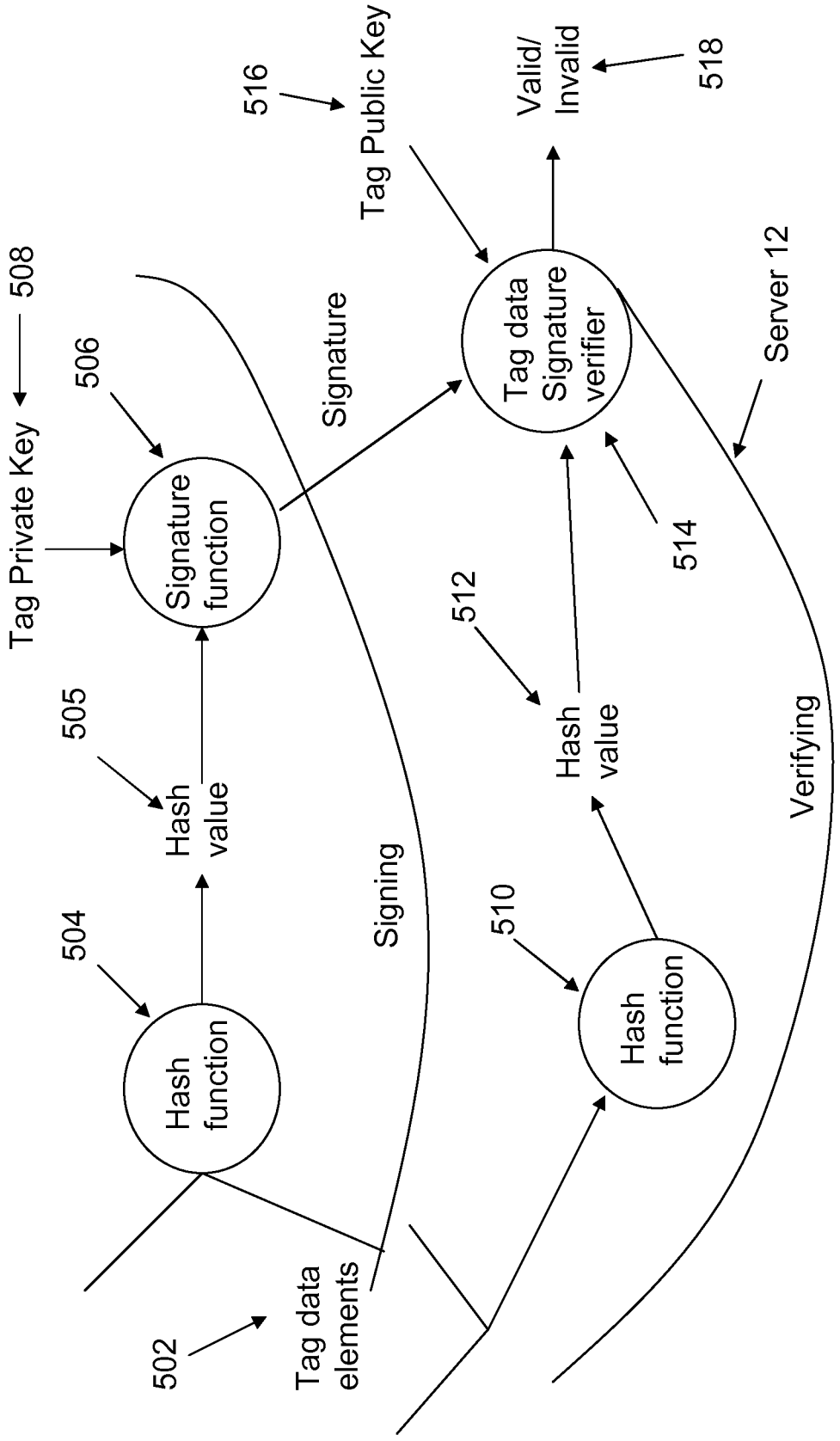

502
Tag data elements
504
Hash function
505
Hash value
506
Signature function
508
Tag Private Key
Signing
Signature
516
Tag Public Key
Tag data Signature verifier
Valid/ Invalid
518
Server 12
510
Hash function
512
Hash value
514
Verifying

Figure 2

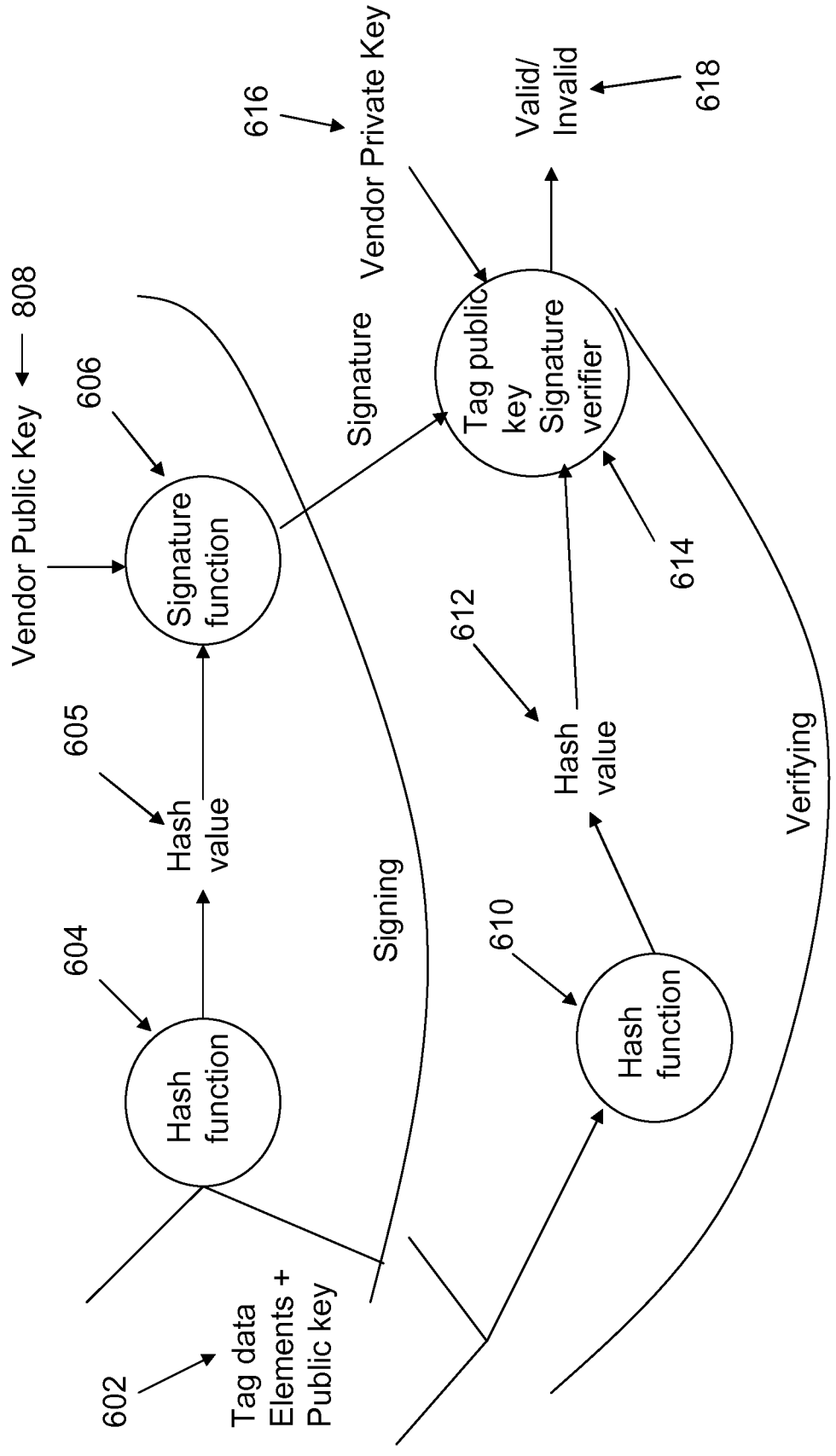
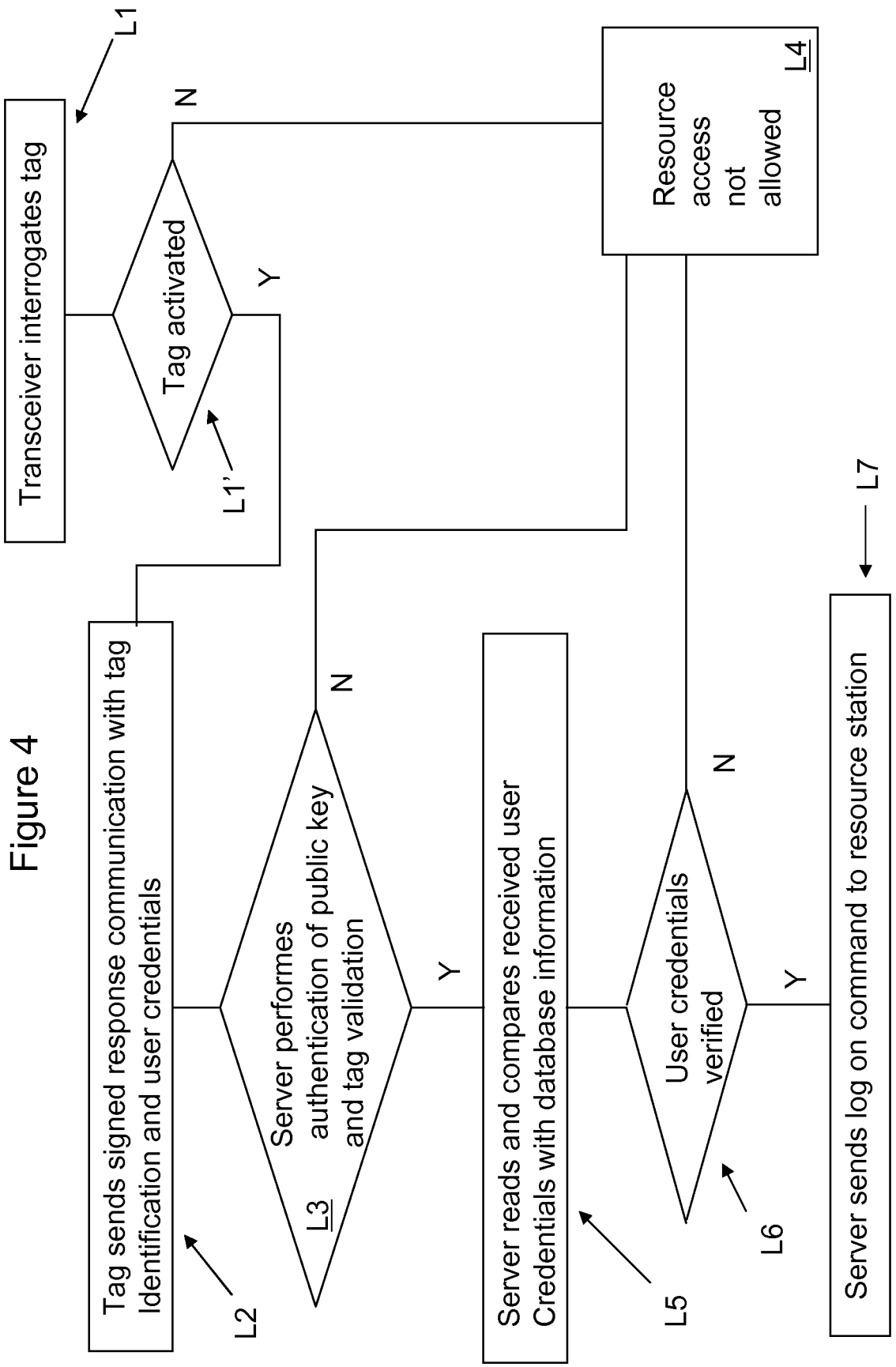

602
Tag data Elements + Public key
604
Hash function
605
Hash value
606
Signature function
Vendor Public Key
808
616
Vendor Private Key
Signature
Signing
610
Hash function
612
Hash value
Tag public key Signature verifier
614
Valid/ Invalid
618
Verifying

Figure 3

Figure 4


Transceiver interrogates tag
L1
Tag activated
N
Y
L1'
Resource access not allowed
L4
Tag sends signed response communication with tag Identification and user credentials
L2
Server performes authentication of public key and tag validation
L3
N
Y
Server reads and compares received user Credentials with database information
L5
User credentials verified
N
Y
L6
Server sends log on command to resource station
L7

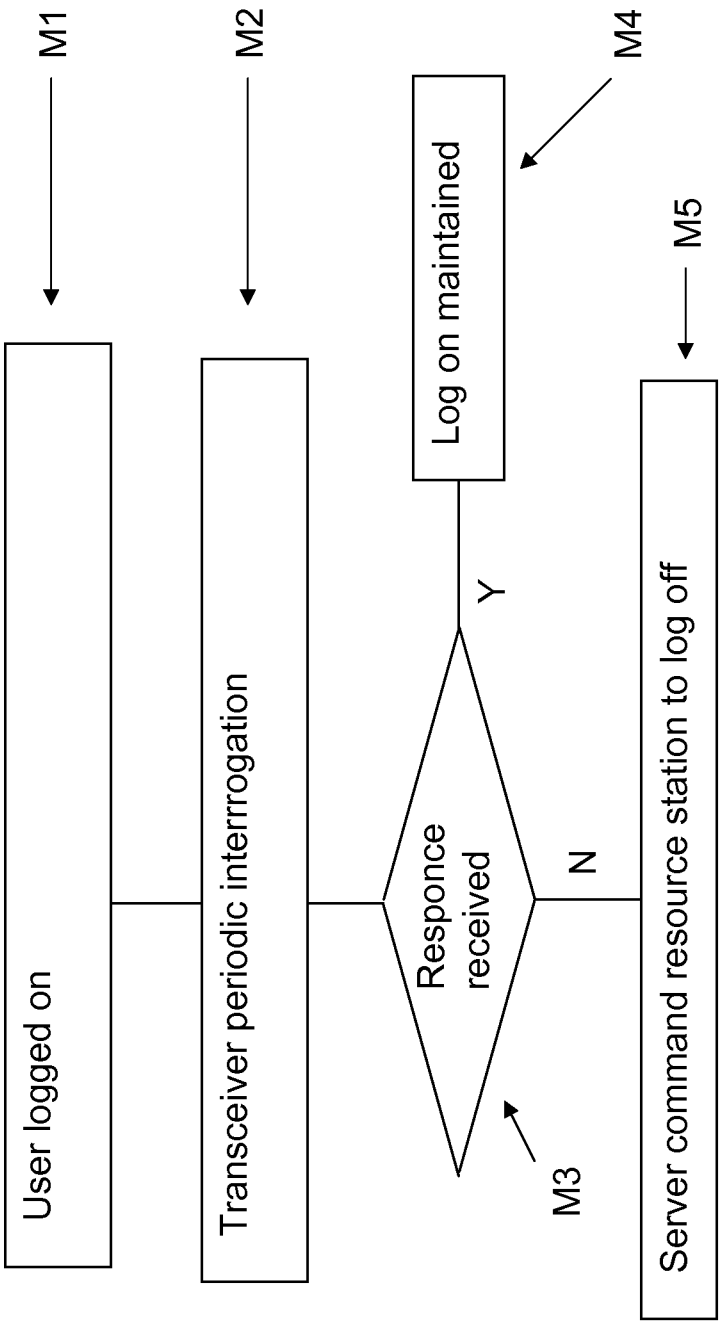

M1
M2
M4
M5
User logged on
Transceiver periodic interrrogation
Log on maintained
Responce received
Y
N
M3
Server command resource station to log off

Figure 5

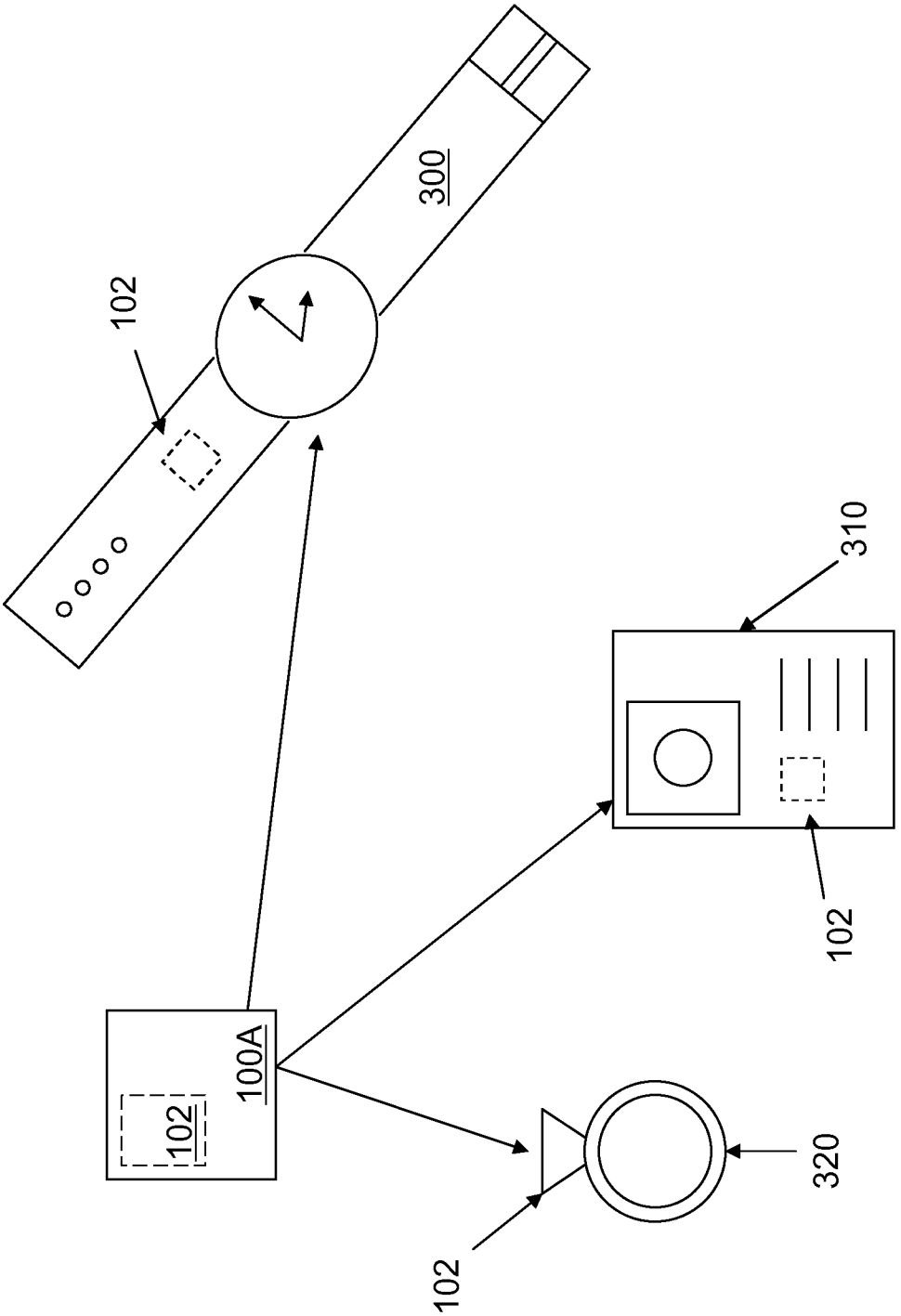


Figure 6

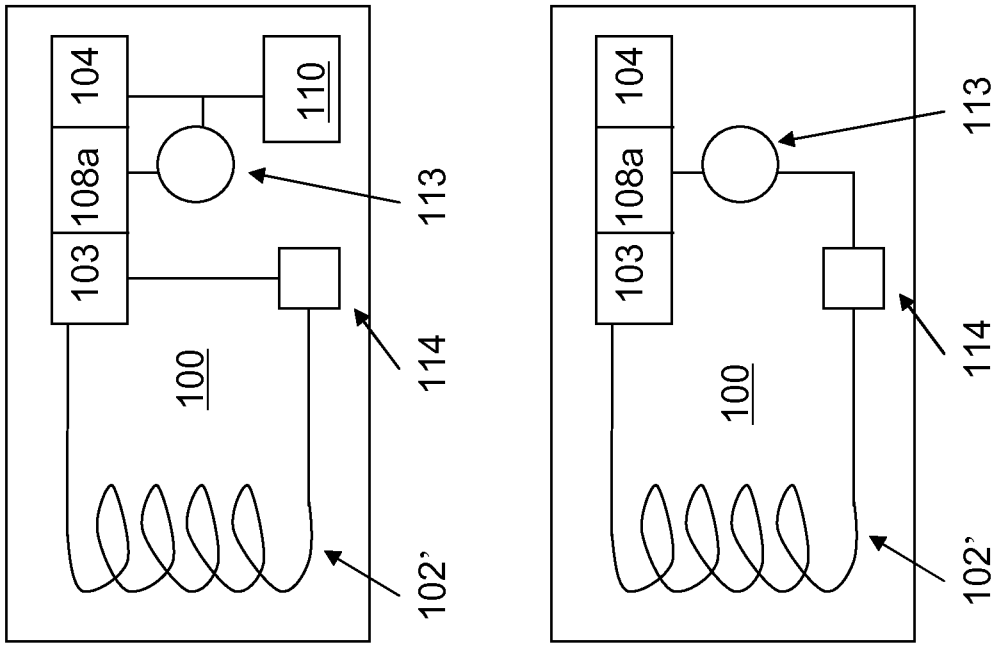


Figure 7